

**Guidelines on preparing a whistleblower policy and example of whistleblower policy**

A company is required to keep written documentation of the establishment of a whistleblower scheme (hereinafter WBS) and the related procedures. Thus, the company must, as a minimum, develop a whistleblower policy and a written procedure for handling reports.

On page 6, we provide an example of a whistleblower policy that can be implemented after a few adaptations. If you want to draw up your own whistleblower policy, the following must or should be considered as a minimum:

**Initial description of the scheme, including purpose and background**

In an introductory section, a general description of the purpose and background for the establishment of the scheme can be provided.

In addition to this, an initial framework may be given for how the company handles employees' affairs, stating that the WBS should function as a supplement to the direct and daily communications in the workplace concerning failings and unsatisfactory matters.

**Who can submit reports?**

A scheme will normally be for use by employees, partners and partners’ employees to report, in good faith, well-founded suspicions and concerns about the company, its employees and partners. Partners associated with the company may, for example, be customers, suppliers or external consultants.

Allowing the scheme to include reporting by former employees, current and former management, and other outside persons may also be considered.

**What can be reported under the scheme?**

The policy should consider which matters can be reported through the scheme, including what may and may not be reported.

The Directive covers the reporting of infringements of a number of EU legal rules. Several countries have indicated that they will also extend the scheme to cover for example, criminal offences, including breach of confidentiality, misuse of funds, theft, fraud, fraudulent conversion, embezzlement and bribery, sexual harassment and other serious harassment at work. Legislation is not yet in place in certain countries. We will update the guide regularly as each country adopts the legislation.

In addition, including other undesirable behaviour in the option for reporting may be considered, depending on the company's circumstances.

In this regard, preparing a positive list and a negative list of matters that fall within and outside the scheme respectively may be considered.

Who can be reported may also be considered. This can usually apply to employees of the company, including management, directors, board members, accountants, lawyers, clients, consultants, suppliers, etc., and other third parties related to the company.

**How should the scheme be organized?**

It should be considered how exactly the scheme is to be organised in the company. The detailed organisation naturally depends on, among other things, the company's location, structure, size, nature and industry.

In this regard, it should be considered who is responsible for receiving reports. There can often be a risk of conflicts of interest, and it will therefore often be appropriate for a company to have reports made to an independent external reporting function that has the necessary expertise and competence to handle all types of report.

It will usually be appropriate to set up a specific team or function in the company, at an appropriate level or with the necessary qualifications, that can work with an external expert to handle the different types of report received.

A manual should be prepared for handling different types of report optimally depending on who is reporting, what is being reported and who is being reported.

**How can reports be made through the scheme?**

In a whistleblower policy, for the sake of potential whistleblowers it should be described precisely how a report can be made through the WBS, including, for example, who provides the IT solution, how it works, which languages can be chosen, whether the report should be made anonymously or by name and other practical matters.

It should also be described how supporting documentation can be submitted and how the communication with a possible whistleblower proceeds.

**What should apply with respect to confidentiality and anonymity?**

A whistleblower policy should describe what applies within the WBS with respect to confidentiality and anonymity. The Act thus provides a special option to process personal data where necessary for handling reports under the scheme. This should be described in a whistleblower policy.

Companies may process non-sensitive data as per GDPR, sensitive personal data and data on criminal offences where necessary to process reports received under the whistleblower scheme.

A whistleblower policy should also state that the other rules and principles of GDPR – which still need to be observed – must also be observed in a whistleblower situation. This also applies in connection with the procedures to be followed in any investigations subsequent to reports. However, it will be possible to disclose the information under certain conditions, including where necessary for the prevention of legal violations, etc.

It can also be stated in a policy that the Act protects whistleblowers against e.g. reprisals when the person in question reports matters with which they have become acquainted in connection with matters relating to their work and the company.

The Act entails that no reprisals may be carried out against whistleblowers, including dismissal, transfer, pay cut, harassment, etc., as a result of them reporting something.

Whistleblowers who have been subjected to reprisals as a result of reporting something are entitled to special compensation.

It should also be stated in a policy how, and according to which procedures, the retention and deletion of personal data are carried out, as well as who is the data controller in relation to the WBS.

**What procedures are follower when a whistleblower reports something?**

A policy should include a description of what procedures apply when a whistleblower reports something. This includes the following:

* how the technical solution works from a whistleblower's perspective,
* deadlines for acknowledging receipt of a report,
* deadlines for receiving feedback,
* guidance for potential whistleblowers on the possibility of reporting via external whistleblower schemes.

A detailed manual should be prepared for internal use in the company in relation to how various reports are to be handled in the collaboration between the company's management, relevant company employees and external experts.

**What are the rights of the persons who are reported?**

A policy should normally describe the rights of persons who have been reported, and there should be a more detailed description of how these employees are to be handled.

The persons to whom the information relates will normally be notified if information is provided about them. The person will thus receive notification when the case is dropped if it is manifestly unfounded, and the person will be involved in the process if the case actually proceeds. In this connection, the person has the right to request correction, deletion or limitation of information.

**What are the rights of the employee who carry out or contribute to investigations?**

The policy should also state the rights of employees who contribute to the whistleblower scheme in connection with investigations that are carried out or information that is provided, including that they are protected against negative employment consequences as a result of their contribution.

**Who can be contacted in case of doubt about the scheme?**

A policy should finally determine who can be contacted in case of doubt about matters concerning the WBS.

**WHISTLEBLOWER POLICY FOR EMPLOYEES   
[to be adapted]**

Last updated (2022)

**Background and purpose**

[NAME OF THE ORGANISATION] (hereinafter “the Organisation”) is making a whistleblower scheme available to our employees.

A whistleblower scheme is an independent channel where employees can report suspicions or specific information about serious violations or other serious matters in the Organisation.

The whistleblower scheme should be seen as a supplement to the opportunity you have as an employee to go to someone in management if you find faults or unsatisfactory matters you want to draw attention to.

This whistleblower policy describes in more detail when you can use the whistleblower scheme, what you can report, how a report is handled, rights for those involved, etc. In addition to this information, the Organisation has drawn up a privacy policy which specifically concerns the processing of personal data in connection with the whistleblower scheme. It can be found here: [insert link].

The whistleblower scheme applies to all employees of the Organisation. It also applies to persons with fixed-term employment or temporary staff.

[Examples of other target groups you might choose to extend the scheme to: board members, shareholders, supervisory board members, consultants, suppliers, contractors, auditors, etc.].

**Who can be reported?**

The whistleblower scheme should be used to report information and matters relating to violations and serious failings by employees or other persons associated with the Organisation. Other persons could be e.g. board members, shareholders, supervisory board members, consultants, suppliers, contractors, auditors, etc.

**What matters can be reported?**

Both violations of EU law, serious violations of national law and other serious matters can be reported, as long as the matters concern persons connected with the Organisation, cf. above.

A report may relate to a suspicion or actual knowledge of violations in, for example, the following areas:

* Public procurement/tendering
* Money laundering and terrorist financing
* Protection of privacy and security of network and information systems
* Consumer protection
* Economic crime, such as embezzlement, theft, bribery, fraud and forgery
* Hacking, tapping, recording conversations between others, etc.
* Violations of legislation on accounting, tax, etc.
* Violations of confidentiality
* Neglect of statutory duty to act
* Violation of rules on the use of force
* Serious and repeated violations of legal principles
* Deliberate deception of citizens and partners
* Physical and psychological violence and sexual abuse or serious harassment based on e.g. race, gender, language, wealth, national or social origin, political or religious affiliation
* Neglect of professional standards that might pose a risk to e.g. the safety and health of persons
* Failure of care
* Serious or repeated violations of the workplace's internal guidelines on e.g. business trips, gifts and financial reporting
* Serious faults and serious irregularities associated with IT operation or IT system management.

The above is a non-exhaustive list of examples.

The whistleblower scheme does not apply to information of a trivial nature or information on e.g. violation of internal guidelines on sick leave, smoking, alcohol, clothing, private use of office supplies, or violation of ancillary rules, such as non-compliance with documentation requirements.

However, in the case of systematic violations, it may well be that these otherwise less serious matters may be covered by the whistleblower scheme. The whistleblower scheme cannot be used to report on your own employment relationship, including conflicts between employees, cooperation issues or matters that come under the system of trade union law (serious harassment and sexual harassment are, however, covered, cf. the above, and cooperation issues are covered if they are deemed to be sufficiently serious to pose a genuine risk to human life and health).

Information on violations or matters that have taken place prior to the Organisation's establishment of a whistleblower scheme may be reported.

**How is a report made?**

The organisation's employees can report anonymously in writing via a digital solution, which is managed by an external supplier.

You will find a link to the whistleblower scheme here: [Insert the link listed at the top of the welcome letter].

Read more about the procedure for reporting here: [insert link to “Guide to using the whistleblowersystem – Whistleblower”].

**Who receives reports?**

Information in a report is received by the Whistleblower Partners Screening Service, which handles reports received via the Organisation's whistleblower scheme. The Whistleblower Partners Screening Service (hereinafter the "Recipient") is an external and independent advisor. When the Recipient has received a report:

* the Recipient screens the report, including for which level at the company the report concerns,
* the Recipient confirms receipt of the report to the whistleblower,
* (*To be adapted depending on the chosen organisation of the whistleblower scheme – delete the whole of section a or b, depending on which is not relevant*)  
    
  (*Covered by the agreement on screening from the* Whistleblower Partners *Screening Service*):  
    
  a. [the Recipient releases the case to the relevant contact person in the Organisation, depending on who is being reported on. Before the Recipient releases the report to the relevant contact person in the Organisation, the Recipient ensures that the report does not concern the relevant contact person and that the relevant contact person has no conflicts of interest in relation to the processing of the report. If this is the case, the report will be shared with another contact person in the Organisation who the Recipient deems competent in relation to the specific report.]  
    
  (Not covered by the agreement on screening from the Whistleblower Partners Screening Service. Requires separate agreement with Whistleblower Partners Get in touch if desired):  
    
  b. [the Recipient handles the issue.]]

We have chosen this particular solution because we want to create the greatest possible sense of security for the Organisation's employees in connection with a report.

**Procedures for receiving a report**

When a report is received, an assessment is made of whether the report falls within the scope of the whistleblower scheme, cf. section 3.

If the report falls outside the scope of the whistleblower scheme, it will be rejected and cannot therefore be handled within the framework of the whistleblower scheme.

If a report falls outside the scope of the whistleblower scheme, the whistleblower will receive guidance on where they can instead raise the matter in question within the Organisation.

**Investigation of a report**

*If solution a. is selected in section 5, insert "the relevant contact person in the Organisation". If solution b. is selected in section 5, insert "Recipient":*

Once [insert] has received the report, [insert] must carry out a thorough follow-up which, depending on the circumstances surrounding the report, may include:

* Initiating an internal investigation to confirm or refute the accuracy of the information in a report
* Briefing the Organisation's top management or board
* Reporting to the police or relevant supervisory authority
* Deciding on responses, e.g. under employment or contract law
* Closing the case

[insert] is responsible for requesting that the report be thoroughly investigated and taking the necessary measures in this regard.

Subsequently, [insert] must prepare a statement for management, which will then decide on the response, whether reporting to the authorities or other responses under employment or contract law.

Finally, feedback must be given to the whistleblower within the 3-month deadline stipulated in the whistleblower scheme, cf. section 10 below.

**Duty of confidentiality and disclosure of information**

Only the Recipient (*Keep if solution 5.a. is selected in section 5:* [and the relevant contact person in the Organisation have]) has access to the information in a report. Reports are subject to a special duty of confidentiality, and the content may therefore not be disclosed to others.

The special duty of confidentiality only applies to information in a report, and if further information emerges as part of a further investigation, such information is not covered by the special duty of confidentiality. For this information, the general rules on disclosure and access to documents apply.

If the whistleblower has waived their anonymity, the special duty of confidentiality no longer applies to the information included in the report. Similarly, the Organisation is entitled to share information from a report, including the identity of the whistleblower, if this is known, with e.g. the police. In such cases, the whistleblower must be informed.

**Anonymity, protection against retaliation and other whistleblower rights**

As a whistleblower, you have the right to remain anonymous throughout the process. The chosen IT solution provides the opportunity to communicate anonymously with the Recipient of the reports.

However, a report may be of such a nature that it can be difficult to thoroughly investigate a matter without the whistleblower choosing to come forward and thus waive their right to anonymity. It is the whistleblower's own decision whether this should happen. If anonymity is waived, the intention of the Whistleblower Directive is to protect the whistleblower from, among other things, any form of retaliation or threat, or attempts at retaliation, that occur as a result of the whistleblower making a report. Retaliation is to be understood as any kind of adverse treatment or adverse consequence that occurs as a reaction to a report. This might e.g. be suspension, dismissal, demotion or lack of promotion, transfer of duties, transfer, pay cut, disciplinary action, coercion, intimidation, harassment, discrimination, etc.

Being mentioned in a report can have significant consequences, and the whistleblower is therefore required to act in good faith regarding the content of a report. A deliberately false report from a whistleblower, e.g. relating to harassment, may lead to criminal consequences for the whistleblower.

On the other hand, a whistleblower cannot be held liable for disclosing confidential information if the whistleblower had reasonable grounds to believe that the information disclosed in the form of a report was correct at the time the report was made and that the information concerned serious violations or other serious matters covered by the scheme.

On this basis, the whistleblower will also not be held responsible for having gained access to the information that has been reported. However, this presupposes that the act by which access was gained does not in itself constitute a criminal act – e.g. burglary.

**Ongoing communication and deadlines**

The recipient handles the communication with the whistleblower via the whistleblower system.

A whistleblower must receive confirmation of receipt of a report no later than 7 days after submitting their report.

In addition, the whistleblower must receive feedback as soon as possible, and no later than 3 months from confirmation of receipt, which means that – to the extent possible – the whistleblower must be informed of what measures have been taken, or are intended to be taken, and why this specific type of follow-up has been chosen. In connection with feedback, some information cannot be shared with the whistleblower, e.g. due to a statutory duty of confidentiality, personal data legislation, etc.

In addition to information about the chosen follow-up, the whistleblower must, to the extent possible, also be given information about the course of the investigation and the outcome, if this can be done within the applicable rules.

If, due to the circumstances of the case, it is not possible to give final feedback before expiry of the 3-month deadline, the whistleblower must be informed of this along with information on when further feedback can be expected.

As mentioned, a whistleblower can choose to come forward, and in that case it may be relevant, for example, to have physical meetings with the Recipient (*Keep if solution a. is selected in section 5:* [and the relevant contact person in the Organisation]).

**Confidentiality**

The whistleblower scheme is designed and managed in such a way as to ensure the confidentiality of the identity of the whistleblower and any persons who may be mentioned in a report.

The IT system used to manage the whistleblower scheme is subject to a number of strict security requirements that, among other things, ensure anonymity and confidentiality. This means that the person making a report via the whistleblower scheme is, and remains, anonymous if desired. It also means that the system does not log IP addresses, that metadata is removed from any uploaded files, and that all data transmission and storage is encrypted.

The Recipient (*Keep if solution a. is selected in section 5:* [and the relevant contact person in the Organisation are]) [is] subject to a duty of confidentiality, and access restrictions have been put in place for all information relating to a report.

**Registration of reports**

Received reports, including the documents included in a report, must be registered (stored systematically) to ensure that the reports are accessible and that, if applicable, they can be used as evidence in any subsequent trial. At the same time, the registration also provides assurance that any reports concerning the same matter are identified and can lead to further investigation of a matter. This registration takes place in the whistleblower system.

Reports are retained for as long as necessary and proportionate. The principles of retention are described in more detail in the Organisation's privacy policy regarding the whistleblower scheme.

**Rights of persons concerned**

Any person mentioned in a report has the right to have their identity protected in connection with the processing of the case. In addition, the affected persons must have access to an effective defence, which is ensured i.e. by registering a report and thus ensuring documentation of the matters mentioned.

The persons concerned also have a number of rights in connection with the processing of their personal data. However, the Organisation's duty of confidentiality entails restrictions in relation to when persons concerned should receive information about the processing of information, and in relation to whether they can invoke right of access, erasure, etc.

If a report leads to a case being brought, the person the report concerns has the right to a consultative procedure or the right to access records concerning the information included in a report. However, if the whistleblower is anonymous, there is no right of access regarding the whistleblower's identity.

**External whistleblower scheme**

Under the Whistleblower Directive, it is the responsibility of the Organisation to inform its employees of the following external whistleblower schemes, which may be used as an alternative to the Organisation's internal scheme:

[Insert description of the national external whistleblower schemes established in the country of the Organisation].

You can find more information on how to make a report through the whistleblower scheme at [Insert name of the organisation responsible for the external whistleblower scheme] here: [Insert link to information on the procedure for reporting to the external whistleblower scheme].

The Organisation's employees have freedom of choice regarding whether to report to the Organisation's internal whistleblower scheme or to an external scheme. However, the Organisation encourages its employees to use the Organisation's own whistleblower scheme in cases where the employee believes that the suspected violation can be handled effectively internally and there is no risk of retaliation.

The option to use either the internal or an external whistleblower scheme does not limit employees' usual freedom of expression.

**The whistleblower´s right of publication**

The Whistleblower Directive and the protection the rules give to whistleblowers also apply to a whistleblower's publication of information mentioned in a report.

However, it is a prerequisite that the whistleblower

* has, prior to publication, made a report both to the Organisation's internal whistleblower scheme and to an external whistleblower scheme without any appropriate action being taken, or
* has reasonable grounds for believing that the violation in question constitutes an imminent or obvious danger to the public interest, or

has reason to believe that reporting to the external whistleblower scheme will entail a risk of retaliation, or that the case will not be dealt with effectively due to its specific circumstances.

**Public disclosure scheme (only keep this section if it´s a public authority)**

As a public authority, the Organisation must, at least once a year, publish a status of reports received in accordance with the Whistleblower Directive, including:

* The number of reports and the overall themes of the reports
* What percentage of the reports
  + have been given active consideration,
  + have been rejected or closed, and
  + have given rise to a report to the police, in absolute terms.